AMENDED IN ASSEMBLY JUNE 15, 2005

AMENDED IN SENATE MAY 11, 2005

AMENDED IN SENATE MAY 4, 2005

AMENDED IN SENATE MARCH 31, 2005

SENATE BILL No. 682

Introduced by Senator Simitian

February 22, 2005

An act to add Article 4 (commencing with Section 1798.9) to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 682, as amended, Simitian. Identity Information Protection Act of 2005.

Existing law, the Information Practices Act of 1977, regulates the collection and disclosure of personal information regarding individuals by state agencies, except as specified. The intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the act is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains.

This bill would enact the Identity Information Protection Act of 2005. The act would ~~prohibit~~ *require* identification documents *that are* created, mandated, purchased, or issued by various public entities ~~from containing~~*, and that contain* a contactless integrated circuit or other device that uses radio waves to broadcast personal information or to enable personal information to be ~~scanned~~ *read* remotely, ~~except as~~ *to meet* specified *requirements*. The bill would provide that ~~its~~

~~provisions do not apply to existing systems, as defined, in use prior to the effective date of this bill~~ *a person or entity that knowingly or willfully remotely reads or attempts to remotely read a person's identification document using radio waves without his or her knowledge shall be punished by imprisonment in a county jail for up to one year, a fine of not more than $5,000, or both that fine and imprisonment*.

~~Because~~ *In addition, because* the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the Information Practices Act of 1977, which would include this act, is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains, and because ~~the scanning~~ *remotely reading* or ~~attempted scanning of~~ *attempting to remotely read* a person's identification document without his or her knowledge would be punishable as a misdemeanor, this bill would create a new crime, thereby imposing a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

SECTION 1. This act shall be known and may be cited as the Identity Information Protection Act of 2005.

SEC. 2. The Legislature hereby finds and declares all of the following:

(a) The right to privacy is a personal and fundamental right protected by Section 1 of Article I of the California Constitution and by the United States Constitution. All individuals have a right of privacy in information pertaining to them.

(b) Easy access to the information found on drivers' licenses and other similar identification documents facilitates the crime of identity theft, a crime that is a major concern in California. More

than 39,000 Californians reported being victims of this crime in 2003.

(c) This state has previously recognized the importance of protecting the confidentiality and privacy of an individual's personal information contained in identification documents such as drivers' licenses.

(d) The inclusion in identification documents of contactless integrated circuits or other devices that use radio waves to broadcast data or to enable data to be scanned secretly and remotely will greatly magnify the potential risk to individual privacy, safety, and ~~economic well-being~~ *financial security* that can occur from unauthorized interception and use of personal information. The inclusion of those devices will also make it possible for any person or entity with access to a reader to engage in the secret tracking of Californians on an unprecedented scale.

SEC. 3. Article 4 (commencing with Section 1798.9) is added to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, to read:

Article 4. Identity Documents

1798.9. For purposes of this article, the following definitions shall apply:

~~(a) "Contactless integrated circuit" means a data carrying unit,~~

(a) "Authentication" means the process of applying a specific mathematical algorithm to data or identification documents, or both, so as to accomplish either of the following:

(1) Prove or establish that the data and the identification document containing the data, including any contactless integrated circuit in the identification document, were issued by the responsible issuing state or local governmental body.

(2) Ensure that a reader, as defined in subdivision (h), is permitted under California law to access such data or identification document.

(b) "Authorized reader" means a reader, as defined in subdivision (h), that, with respect to a particular identification document, (1) is permitted under California law to remotely read the personal information broadcast or transmitted by that identification document, (2) is being used for a lawful purpose,

and (3) is fully in accord with the requirements of subdivision (a) of Section 1798.10.

(c) "Contactless integrated circuit" means a data carrying unit, such as an integrated circuit or computer chip, that can be read remotely.

(d) "Encryption" means the process of applying a specific mathematical algorithm to data so as to protect the confidentiality of that data by rendering that data unintelligible to an unauthorized party.

(e) "Identification document" means any document containing personal information that an individual uses alone or in conjunction with any other information to establish his or her identity. Identification documents specifically include, but are not limited to, the following:

(1) Driver's licenses or identification cards.

(2) Identification cards for employees or contractors.

(3) Identification cards issued by educational institutions.

(4) Health insurance or benefit cards.

(5) Benefit cards issued in conjunction with any government-supported aid program.

(6) Licenses, certificates, registration, or other means to engage in a business or profession regulated by the Business and Professions Code.

(7) Library cards issued by any public library.

(f) "Mutual authentication" means the use of authentication, as defined in subdivision (a), to ensure that authorized readers, as defined in subdivision (b), can reliably detect unauthorized identification documents, and that authorized identification documents can be read only by those authorized readers.

(g) "Personal information" includes any of the following: an individual's name, address, telephone number, e-mail address, date of birth, religion, ethnicity, nationality, photograph, fingerprint or other biometric identification, social security number, or any other unique personal identifier or number.

(h) "Reader" means a scanning device that is capable of using radio waves to communicate with a contactless integrated circuit or other device using radio waves and read the personal information broadcast or transmitted by that integrated circuit or other device.

(i) "Remotely" means that no physical contact between the integrated circuit or device and a reader is necessary in order to transmit data.

(j) "Shield devices" mean physical or technological protections available to stop the broadcast or transmission of personal information programmed on or into a contactless integrated circuit or other devices using radio waves.

(k) "Unique identifier number" means a random string of numbers that is encoded onto the contactless integrated circuit or other device.

1798.10. (a) Except as provided in subdivisions (b) and (c) all identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof that contain a contactless integrated circuit or other device that uses radio waves to broadcast personal information or to enable personal information to be read remotely shall meet these requirements:

(1) The identification document shall not contain, transmit, or enable the remote reading of, any personal information other than a unique personal identifier number in or from its contactless integrated circuit or other device that uses radio waves.

(2) The identification document shall implement strong encryption to protect against the unauthorized reading of transmitted information. The confidentiality provided by that encryption shall at all times be at least as strong as RSA encryption using a key length of 1024 bit as understood on the effective date of this article. In the event that this standard is cracked and hence no longer capable of protecting against the unauthorized reading of transmitted information, the identification document shall implement a stronger encryption standard that will ensure protection against the unauthorized reading of transmitted information.

(3) The identification document shall implement mutual authentication to protect against the unauthorized transmission of information from the identification document to unauthorized readers. The protection provided by that mutual authentication shall at all times and at a minimum incorporate the highest standards of active mutual authentication contained in Common Criteria ISO 15408 or its equivalent as subsequently updated.

The identification document shall in no case incorporate a lower standard for active mutual authentication than the highest standard articulated by Common Criteria ISO 15408 at the time of the effective date of this article.

(4) In order to ensure that the holder of the identification document affirmatively consents to each reading of the identification document, each identification document shall implement at least one of the following privacy safeguards:

(A) An access control protocol requiring the optical or other non-radio frequency reading of information from the identification document prior to each transmission or broadcast of data using radio waves, without which the identification document will not transmit or broadcast personal information using radio waves.

(B) A shield device that, when used to protect the identification document, can prevent any communication of data using radio waves between the contactless integrated circuit and any reader under any circumstances.

(C) A contactless integrated circuit or other device that is normally not remotely readable, accessible, or otherwise operational under any circumstances, and only remotely readable, accessible, or operational while being temporarily switched on or otherwise intentionally activated by a person in physical possession of the identification document. Any such device must only be remotely readable while the person intentionally uses the switch intending that the identification document be read.

(5) The issuing entity of an identification document shall communicate in writing to the person to whom the document is issued, all of the following:

(A) That the identification document contains a contactless integrated circuit or device that can broadcast a unique personal identifier number or enable that number to be read remotely without his or her knowledge.

(B) That countermeasures, such as shield devices, may be used to help the person control the risk that his or her unique personal identifier number will be broadcast or read remotely without his or her knowledge.

(C) The location of all readers used or intended to be used by the issuing authority or by any other entity known to that

authority to read the unique personal identifier number on the identification document.

(D) Any information that is being collected at the time the contactless integrated circuit or other device is read or that is being stored regarding the individual in a database.

(E) Additional annual notice shall be communicated in writing of any new shield devices in existence or changes in the location of readers or the information collected or stored in the database.

(b) Subdivision (a) shall not apply to:

(1) An identification document that is part of a contactless integrated system used by a state, county, or municipal government, or subdivision or agency thereof that is operational and in use prior to January 1, 2006, if all of the following apply:

(A) The system is not used for any purpose other than the purpose or purposes of the system on the effective date of this article.

(B) The amount, type, or types of information stored, broadcast, or transmitted by the contactless integrated circuit is the same as, or less or fewer than, on the effective date of this article.

(C) The contactless integrated circuit is being issued to the same group or groups as, or fewer or smaller groups of people than, were issued the contactless integrated circuit on the effective date of this article.

(2) An identification document issued to a person who is incarcerated in the state prison or a county jail, detained in a juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation, or housed in a mental health facility, pursuant to a court order after having been charged with a crime, or to a person pursuant to court-ordered electronic monitoring.

(3) An identification document issued to a person employed by a state prison, county jail, or juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation if the document is not removed from the facility and the requirements of paragraph (4) of subdivision (a) apply.

(4) An identification document issued to a firefighter if the document is used only while the firefighter is on active duty and the requirements of paragraph (4) of subdivision (a) apply.

(5) An identification document issued to a patient who is in the care of a government-operated hospital, ambulatory surgery center, or oncology or dialysis clinic if the document is (1) valid for only a single episode of care, (2) removed from the patient at the time the patient is discharged, and (3) contains no personal information other than a unique identifier number, and a patient returning for a new episode of care is assigned a new unique identifier number.

(6) An identification document issued to a patient by emergency medical services for triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly related to a disaster, as defined by the local Emergency Medical Services agency organized under Section 1797.200 of the Health and Safety Code.

(c) Except for identification documents listed in subdivision (b), the following identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof, shall not contain a contactless integrated circuit or other device that uses radio waves to broadcast personal information or to enable personal information to be read remotely:

(1) Drivers' licenses or identification cards.

(2) Identification cards issued to students by educational institutions, including but not limited to, all K-12 schools, the University of California, California State Universities, and the community colleges.

(3) Health insurance, health benefit, and benefit cards issued in conjunction with any government-supported aid program.

(4) Library cards issued by any public library.

1798.12. A person or entity that knowingly or willfully remotely reads or attempts to remotely read a person's identification document using radio waves, without the knowledge of that person shall be punished by imprisonment in a county jail for up to one year, a fine of not more than five thousand dollars ($5,000), or both that fine and imprisonment.

SEC. 4. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the

penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

~~such as an integrated circuit or computer chip, that can be read remotely.~~

~~(b) "Identification document" means any document containing personal information that an individual uses alone or in conjunction with any other information to establish his or her identity. Identification documents specifically include, but are not limited to, the following:~~

~~(1) Driver's licenses or identification cards.~~

~~(2) Identification cards for employees or contractors.~~

~~(3) Identification cards issued by educational institutions.~~

~~(4) Health insurance or benefit cards.~~

~~(5) Benefit cards issued in conjunction with any government-supported aid program.~~

~~(6) Licenses, certificates, registration, or other means to engage in a business or profession regulated by the California Business and Professions Code.~~

~~(7) Library cards issued by any public library.~~

~~(c) "Personal information" includes any of the following: an individual's name, address, telephone number, e-mail address, date of birth, race, religion, ethnicity, nationality, photograph, fingerprint or other biometric identification, social security number, or any other unique personal identifier or number.~~

~~(d) "Remotely" means that no physical contact between the integrated circuit or device and a reader is necessary in order to transmit data.~~

~~1798.10. The identification document created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof shall not contain a contactless integrated circuit or other device that uses radio waves to broadcast personal information or to enable personal information to be scanned remotely, except for the following:~~

~~(a) The identification document is to be used on a toll road or bridge for the specific purpose of collecting funds for the use of that road or bridge, such as FasTrak.~~

~~(b) The identification document is to be given to a person who is incarcerated in the state prison or a county jail, detained in a~~

~~juvenile facility operated by the California Youth Authority, or housed in a mental health facility, pursuant to a court order after having been charged with a crime, or to a person pursuant to court-ordered electronic monitoring.~~

~~(c) The identification document is to be given to a child four years of age or younger who is in the custodial care of a government-operated hospital, clinic, or other medical facility.~~

~~(d) The identification document is to be given to a patient who is in the care of a government-operated hospital, ambulatory surgery center, or oncology or dialysis clinic, but the identification document is valid for only a single episode of care and is removed from the patient at the time the patient is discharged. A patient returning for a new episode of care shall be assigned a new unique identifier number.~~

~~(e) The identification document is issued for the purpose of facilitating secured access by the identification document holder to a secured public building.~~

~~(f) The identification document is part of a contactless integrated system used by a state, county, or municipal government, or subdivision or agency thereof that is operational and in use prior to January 1, 2006.~~

~~(g) The Legislature determines through legislation that an exception allowing the inclusion of a contactless integrated circuit or other device is necessary to meet a compelling state interest and that there exists no means less intrusive to the individual's privacy and security that would achieve that compelling state interest.~~

~~1798.10.5. An identification document described in subdivisions (a) to (e), inclusive, or (g), of Section 1798.10 shall not contain, transmit, or enable the remote scanning of, any personal information other than a unique personal identifier number.~~

~~1798.11. The issuing entity of an identification document described in subdivision (a), (d), (e), or (g) of Section 1798.10 shall communicate in writing to the person to whom the document is issued, all of the following:~~

~~(a) That the identification document contains a circuit or device that can broadcast a unique personal identifier number or enable that number to be scanned remotely without his or her knowledge.~~

~~(b) That countermeasures, such as shield devices, may be used to help one control the risk that his or her unique personal identifier number will be broadcast or scanned remotely without his or her knowledge.~~

~~(c) The location of all scanners and readers used or intended to be used by the issuing authority or by any other entity known to that authority to read the unique personal identifier number on the identification document.~~

~~1798.12. A person or entity that, using radio waves, remotely scans or attempts to remotely scan a person's identification document without the knowledge of that person may be punished, upon conviction, by imprisonment in a county jail for up to one year. The court may also impose a fine of no more than five thousand dollars ($5,000), or may impose both imprisonment and fine.~~

~~1798.12.5. This act shall not apply to existing systems in use prior to the effective date of this article. For purposes of this section, "system" means a network of contactless integrated circuits and corresponding scanners issued by an entity for a limited purpose or purposes.~~

~~SEC. 4. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.~~

O